

HOUSE BILL NO. 1339

AMENDMENT IN THE NATURE OF A SUBSTITUTE

(Proposed by the House Committee on Public Safety

on _____)

(Patron Prior to Substitute--Delegate Leftwich)

A BILL to amend and reenact §§ 15.2-1723.2 and 23.1-815.1 of the Code of Virginia and to amend the Code of Virginia by adding a section numbered 52-4.5, relating to facial recognition technology; Department of State Police and authorized uses.

Be it enacted by the General Assembly of Virginia:

1. That §§ 15.2-1723.2 and 23.1-815.1 of the Code of Virginia are amended and reenacted and that the Code of Virginia is amended by adding a section numbered 52-4.5 as follows:

§ 15.2-1723.2. Facial recognition technology; approval.

A. For purposes of this section, ~~"facial;~~

"Authorized use" means the use of facial recognition technology to (i) help identify an individual when there is a reasonable suspicion the individual has committed, is committing, or is planning the commission of a crime; (ii) help identify a crime victim, including a victim of online sexual abuse material; (iii) help identify a person who may be a missing person or witness to criminal activity; (iv) help identify a victim of human trafficking or an individual involved in the trafficking of humans, weapons, drugs, or wildlife; (v) help identify an online recruiter of criminal activity, including but not limited to human, weapon, drug, and wildlife trafficking; (vi) help a person who is suffering from a mental or physical disability impairing his ability to communicate and be understood; (vii) help identify a deceased person; (viii) help identify a person who is incapacitated or otherwise unable to identify himself; (ix) help identify a person who is reasonably believed to be a danger to himself or others; (x) help identify an individual lawfully detained; (xi) help mitigate an imminent threat to public safety, a significant threat to life, or a threat to national security, including acts of terrorism; (xii) ensure officer safety as part of the vetting of undercover law enforcement; (xiii) determine whether an individual may have unlawfully obtained one or

27 more state driver's licenses, financial instruments, or other official forms of identification using
28 information that is fictitious or associated with a victim of identity theft; or (xiv) help identify a person
29 who an officer reasonably believes is concealing his true identity and about whom the officer has a
30 reasonable suspicion has committed a crime other than concealing his identity.

31 "Facial recognition technology" means an electronic system or service for enrolling, capturing,
32 extracting, comparing, and matching an individual's geometric facial data to identify individuals in photos,
33 videos, or real time conducting an algorithmic comparison of images of a person's facial features for the
34 purpose of identification. "Facial recognition technology" does not include the use of an automated or
35 semi-automated process to redact a recording in order to protect the privacy of a subject depicted in the
36 recording prior to release or disclosure of the recording outside of the law-enforcement agency if the
37 process does not generate or result in the retention of any biometric data or surveillance information.

38 "Publicly post" means to post on a website that is maintained by the entity or on any other website
39 on which the entity generally posts information and that is available to the public or that clearly describes
40 how the public may access such data.

41 "State Police Model Facial Recognition Technology Policy" means the model policy developed
42 and published by the Department of State Police pursuant to § 52-4.5.

43 B. No Pursuant to § 2.2-1112, the Division of Purchases and Supply (the Division) shall determine
44 the appropriate facial recognition technology for use in accordance with this section. The Division shall
45 not approve any facial recognition technology unless it has been evaluated by the National Institute of
46 Standards and Technology (NIST) as part of the Face Recognition Vendor Test. Any facial recognition
47 technology utilized shall utilize algorithms that have demonstrated (i) an accuracy score of at least 98
48 percent true positives within one or more datasets relevant to the application in a NIST Facial Recognition
49 Vendor Test report and (ii) minimal performance variations across demographics associated with race,
50 skin tone, ethnicity, or gender. The Division shall require all approved vendors to annually provide
51 independent assessments and benchmarks offered by NIST to confirm continued compliance with this
52 section.

53 C. A local law-enforcement agency shall purchase or deploy may use facial recognition technology
54 unless such purchase or deployment of facial recognition technology is expressly authorized by statute for
55 authorized uses. For purposes of this section, a statute that does not refer to facial recognition technology
56 shall not be construed to provide express authorization. Such statute shall require that any facial
57 recognition technology purchased or deployed by the local law enforcement agency be maintained under
58 the exclusive control of such local law enforcement agency and that any data contained by such facial
59 recognition technology be kept confidential, not be disseminated or resold, and be accessible only by a
60 search warrant issued pursuant to Chapter 5 (§ 19.2 52 et seq.) of Title 19.2 or an administrative or
61 inspection warrant issued pursuant to law. A match made through facial recognition technology shall not
62 constitute probable cause for an arrest but shall be admissible as exculpatory evidence.

63 C-D. A local law-enforcement agency shall publicly post and annually update its policy regarding
64 the use of facial recognition technology before employing such facial recognition technology to
65 investigate a specific criminal incident or citizen welfare situation. A local law-enforcement agency that
66 uses facial recognition technology may adopt the State Police Model Facial Recognition Technology
67 Policy. If a local law-enforcement agency uses facial recognition technology but does not adopt such
68 model policy, such agency shall develop its own policy within 90 days of publication of the State Police
69 Model Facial Recognition Technology Policy that meets or exceeds the standards set forth in such model
70 policy.

71 E. Any local law-enforcement agency that uses facial recognition technology shall maintain
72 records sufficient to facilitate discovery in criminal proceedings, post-conviction proceedings, public
73 reporting, and auditing of compliance with such agency's facial recognition technology policies. Such
74 agency shall collect data pertaining to (i) a complete history of each user's queries; (ii) the total number
75 of queries conducted; (iii) the number of queries that resulted in a list of possible candidates; (iv) how
76 many times an examiner offered law enforcement an investigative lead based on his findings; (v) how
77 many cases were closed due to an investigative lead from facial recognition technology; (vi) what types
78 of criminal offenses are being investigated; (vii) the nature of the image repository being compared or
79 queried; and (viii) if applicable, any other entities with which the agency shared facial recognition data.

80 F. Any chief of police whose agency uses facial recognition technology shall publicly post and
81 annually update a report by April 1 each year to provide information to the public regarding the agency's
82 use of facial recognition technology. The report shall include all data required by clauses (ii) through (viii)
83 of subsection E in addition to (i) all instances of unauthorized access of the facial recognition technology,
84 including any unauthorized access by employees of the agency; (ii) vendor information, including the
85 specific algorithms employed; and (iii) if applicable, data or links related to third-party testing of such
86 algorithms, including any reference to variations in demographic performance. If any information or data
87 (a) contains an articulable concern for any person's safety, (b) is otherwise prohibited from public
88 disclosure by federal or state statute, or (c) if disclosed, may compromise sensitive criminal justice
89 information, such information or data may be excluded from public disclosure. Nothing herein shall limit
90 disclosure of data collected pursuant to subsection E when such disclosure is related to a writ of habeas
91 corpus.

92 For purposes of this subsection, "sensitive criminal justice information" means information related
93 to (1) a particular ongoing criminal investigation or proceeding, (2) the identity of a confidential source,
94 or (3) law-enforcement investigative techniques and procedures.

95 G. At least 30 days prior to procuring facial recognition technology, a local law-enforcement
96 agency shall notify in writing the governing body of the locality that such agency serves of such intended
97 procurement, but such notice shall not be required if such procurement is directed by the governing body.

98 H. Nothing in this section shall apply to commercial air service airports.

99 **§ 23.1-815.1. Facial recognition technology; approval.**

100 A. For purposes of this subsection, "facial section":

101 "Authorized use" means the use of facial recognition technology to (i) help identify an individual
102 when there is a reasonable suspicion the individual has committed, is committing, or is planning the
103 commission of a crime; (ii) help identify a crime victim, including a victim of online sexual abuse material;
104 (iii) help identify a person who may be a missing person or witness to criminal activity; (iv) help identify
105 a victim of human trafficking or an individual involved in the trafficking of humans, weapons, drugs, or
106 wildlife; (v) help identify an online recruiter of criminal activity, including but not limited to human,

107 weapon, drug, and wildlife trafficking; (vi) help a person who is suffering from a mental or physical
108 disability impairing the person's ability to communicate and be understood; (vii) help identify a deceased
109 person; (viii) help identify a person who is incapacitated or otherwise unable to identify himself; (ix) help
110 identify a person who is reasonably believed to be a danger to himself or others; (x) help identify an
111 individual lawfully detained; (xi) help mitigate an imminent threat to public safety, a significant threat to
112 life, or a threat to national security, including acts of terrorism; (xii) ensure officer safety as part of the
113 vetting of undercover law enforcement; (xiii) determine whether an individual may have unlawfully
114 obtained one or more state driver's licenses, financial instruments, or other official forms of identification
115 using information that is fictitious or associated with a victim of identity theft; or (xiv) help identify a
116 person who an officer reasonably believes is concealing his true identity and about whom the officer has
117 a reasonable suspicion has committed a crime other than concealing his identity.

118 "Facial recognition technology" means an electronic system or service for enrolling, capturing,
119 extracting, comparing, and matching an individual's geometric facial data to identify individuals in photos,
120 videos, or real time conducting an algorithmic comparison of images of a person's facial features for the
121 purpose of identification. "Facial recognition technology" does not include the use of an automated or
122 semi-automated process to redact a recording in order to protect the privacy of a subject depicted in the
123 recording prior to release or disclosure of the recording outside of the law-enforcement agency if the
124 process does not generate or result in the retention of any biometric data or surveillance information.

125 "Publicly post" means to post on a website that is maintained by the entity or on any other website
126 on which the entity generally posts information and that is available to the public or that clearly describes
127 how the public may access such data.

128 "State Police Model Facial Recognition Technology Policy" means the model policy developed
129 and published by the Department of State Police pursuant to § 52-4.5.

130 B. ~~No~~ Pursuant to § 2.2-1112, the Division of Purchases and Supply (the Division) shall determine
131 the appropriate facial recognition technology for use in accordance with this section. The Division shall
132 not approve any facial recognition technology unless it has been evaluated by the National Institute of
133 Standards and Technology (NIST) as part of the Face Recognition Vendor Test. Any facial recognition

134 technology utilized shall utilize algorithms that have demonstrated (i) an accuracy score of at least 98
135 percent true positives within one or more datasets relevant to the application in a NIST Facial Recognition
136 Vendor Test report, and (ii) minimal performance variations across demographics associated with race,
137 skin tone, ethnicity, or gender. The Division shall require all approved vendors to annually provide
138 independent assessments and benchmarks offered by NIST to confirm continued compliance with this
139 section.

140 C. A campus police department shall purchase or deploy may use facial recognition technology
141 unless such purchase or deployment of facial recognition technology is expressly authorized by statute for
142 authorized uses. For purposes of this section, a statute that does not refer to facial recognition technology
143 shall not be construed to provide express authorization. Such statute shall require that any facial
144 recognition technology purchased or deployed by the campus police department be maintained under the
145 exclusive control of such campus police department and that any data contained by such facial recognition
146 technology be kept confidential, not be disseminated or resold, and be accessible only by a search warrant
147 issued pursuant to Chapter 5 (§ 19.2-52 et seq.) of Title 19.2 or an administrative or inspection warrant
148 issued pursuant to law. A match made through facial recognition technology shall not constitute probable
149 cause for an arrest but shall be admissible as exculpatory evidence.

150 D. A campus police department shall publicly post its policy on use of facial recognition
151 technology before employing such facial recognition technology to investigate a specific criminal incident
152 or citizen welfare situation. A campus police department that uses facial recognition technology may adopt
153 the State Police Model Facial Recognition Technology Policy. If a campus police department uses facial
154 recognition technology but does not adopt the State Police Model Facial Recognition Technology Policy,
155 such department shall develop its own policy within 90 days of publication of the State Police Model
156 Facial Recognition Technology Policy that meets or exceeds the standards set forth in such model policy.
157 Any policy adopted or developed pursuant to this subsection shall be updated annually.

158 E. Any campus police department that uses facial recognition technology shall maintain records
159 sufficient to facilitate discovery in criminal proceedings, post-conviction proceedings, public reporting,
160 and auditing of compliance with such department's facial recognition technology policies. Such

161 department that uses facial recognition technology shall collect data pertaining to (i) a complete history
162 of each user's queries; (ii) the total number of queries conducted; (iii) the number of queries that resulted
163 in a list of possible candidates; (iv) how many times an examiner offered campus police an investigative
164 lead based on his findings; (v) how many cases were closed due to an investigative lead from facial
165 recognition technology; (vi) what types of criminal offenses are being investigated; (vii) the nature of the
166 image repository being compared or queried; and (viii) if applicable, any other entities with which the
167 department shared facial recognition data.

168 F. Any chief of a campus police department whose agency uses facial recognition technology shall
169 publicly post and annually update a report by April 1 each year to provide information to the public
170 regarding the agency's use of facial recognition technology. The report shall include all data required by
171 clauses (ii) through (viii) of subsection E in addition to (i) all instances of unauthorized access of the facial
172 recognition technology, including any unauthorized access by employees of the campus police
173 department; (ii) vendor information, including the specific algorithms employed; and (iii) if applicable,
174 data or links related to third-party testing of such algorithms, including any reference to variations in
175 demographic performance. If any information or data (a) contains an articulable concern for any person's
176 safety, (b) is otherwise prohibited from public disclosure by federal or state statute, or (c) if disclosed,
177 may compromise sensitive criminal justice information, such information or data may be excluded from
178 public disclosure. Nothing herein shall limit disclosure of data collected pursuant to subsection E when
179 such disclosure is related to a writ of habeas corpus.

180 For purposes of this subsection, "sensitive criminal justice information" means information related
181 to (1) a particular ongoing criminal investigation or proceeding, (2) the identity of a confidential source,
182 or (3) law-enforcement investigative techniques and procedures.

183 G. At least 30 days prior to procuring facial recognition technology, a campus police department
184 shall notify in writing the institution of higher education that such department serves of such intended
185 procurement, but such notice shall not be required if such procurement is directed by the governing body.

186 **§ 52-4.5. Department to establish a State Police Model Facial Recognition Technology Policy.**

